

# (12) UK Patent Application (19) GB (11) 2 376 764 (13) A

(43) Date of A Publication 24.12.2002

(21) Application No 0114891.5

(22) Date of Filing 19.06.2001

(71) Applicant(s)

Hewlett-Packard Company  
(Incorporated in USA - Delaware)  
3000 Hanover Street, Palo Alto,  
California 94304, United States of America

(72) Inventor(s)

Liqun Chen  
Michael Child  
Christopher I Dalton  
Jonathan Griffin  
Andrew Patrick Norman

(74) Agent and/or Address for Service

Richard Anthony Lawrence  
Hewlett-Packard Limited, IP Section,  
Filton Road, Stoke Gifford, BRISTOL,  
BS34 8QZ, United Kingdom

(51) INT CL<sup>7</sup>

G06F 1/00

(52) UK CL (Edition T )

G4A AAP

(56) Documents Cited

EP 1030237 A1

WO 2000/048063 A1

(58) Field of Search

UK CL (Edition T ) G4A AAP

INT CL<sup>7</sup> G06F 1/00 9/455 12/14

Other: ONLINE:WPI,EPODOC,JAPIO,TDB,  
INSPEC,XPESP

(54) Abstract Title

**A trusted computing environment with an integrity metric for both host and guest operating systems**

(57) A computing platform 20 provides multiple computing environments 24 each containing a guest operating system 25 provided by a virtual machine application 26. Optionally, each computing environment 24 is formed in a compartment 220 of a compartmented host operating system 22. A trusted device 213 verifies that the host operating system 22 and each guest operating system 25 operates in a secure and trusted manner by forming integrity metrics which can be interrogated by a user 10. Each computing environment is isolated and secure, and can be verified as trustworthy independent of any other computing environment.

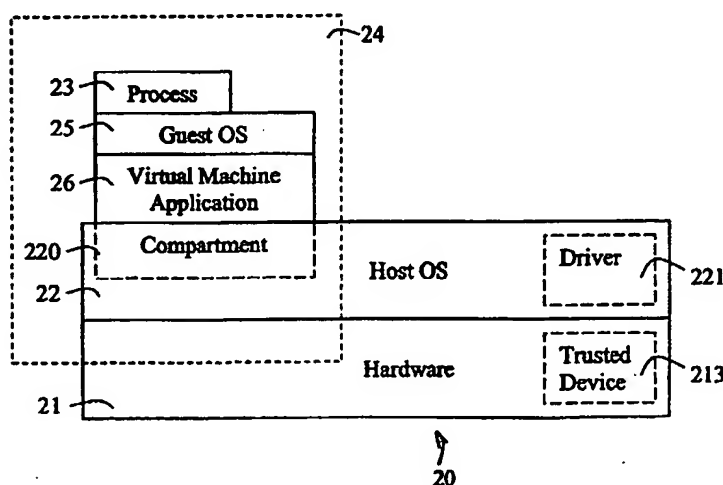


Fig. 2

GB 2 376 764 A

### Multiple Trusted Computing Environments

The present invention relates in general to a method for providing multiple computing environments running on a single host computing platform, and relates to a method  
5 for verifying integrity of the computing environments.

It is desired to run multiple applications on a single host computing platform such as a server. It is known to  
10 provide a separate logically distinct computing environment for each application. However, a problem arises when one application or its environment is incompatible with another application, or is not considered trusted by another application.

15

An aim of the present invention is to provide a method that allows multiple computing environments to be provided on a single host computing platform. A preferred aim is to provide a high degree of isolation between the multiple  
20 computing environments. Another preferred aim is to provide a method for verifying integrity of one computing environment independently of any other of the computing environments, such that each environment is independently trustworthy.

25

According to a first aspect of the present invention there is provided a method for providing a trusted computing environment, comprising the steps of: (a) providing a host operating system; (b) obtaining an  
30 integrity metric for the host operating system; (c) providing a computing environment including a guest operating system; and (d) obtaining an integrity metric for the computing environment.

Preferably, the step (b) includes obtaining the integrity metric during boot of the host operating system. Preferably, the step (b) includes obtaining an integrity metric for a BIOS and/or an OS loader and/or an operating system software of the host operating system. Preferably, the step (b) includes obtaining the integrity metric by performing data event logging, and/or by performing a hash function to all or selected data files associated with the host operating system. Preferably, the step (b) comprises updating at least part of the integrity metric for the host operating system.

Additionally, the step (d) comprises obtaining an integrity metric of the guest operating system. Suitably, the step (c) comprises providing a virtual machine application running on the host operating system for providing the guest operating system. Preferably, the step (d) comprises obtaining an integrity metric of the virtual machine application. Further, the step (c) comprises providing a process running on the guest operating system. Preferably, the step (d) comprises obtaining an integrity metric of the process.

In the preferred embodiments of the invention, the step (c) comprises providing the computing environment in a compartment of the host operating system. Preferably, the host operating system is a compartmented operating system. Suitably, the compartment confines the guest operating system. It is preferred that the step (d) comprises obtaining an integrity metric from a history of all processes launched in the compartment.

Preferably, the step (d) comprises updating at least part of the integrity metric for the computing environment. Preferably, the step (b) comprises storing the integrity metric for the host operating system, and/or  
5 the step (d) comprises storing the integrity metric for the computing environment. Preferably, the integrity metric for the computing environment is stored associated with an identity of the computing environment.

10 Preferably, the step (b) and/or the step (d) comprises obtaining the integrity metric using a trusted device, and storing the integrity metric in a platform configuration register of the trusted device. Preferably, the integrity metric for the computing environment is stored in a  
15 platform configuration register or group of platform configuration registers associated with the computing environment.

Additionally, the method preferably comprises the step  
20 of verifying the trusted computing environment including the steps of: (e) identifying the computing environment; (f) supplying the integrity metric for the host operating system; and (g) supplying the integrity metric for the computing environment.

25

Although the present invention has been introduced above in terms of a single computing environment, preferably a plurality of computing environments are provided on a single host computing platform. Suitably,  
30 the step (c) comprises providing a plurality of computing environments each including a guest operating system, and the step (d) comprises obtaining an integrity metric of each computing environment.

According to a second aspect of the present invention there is provided a method for verifying integrity of a trusted computing environment amongst many on a single host computing platform running a host operating system, each computing environment comprising a guest operating system running on the host operating system, the method comprising the steps of: (a) identifying the computing environment; (b) supplying an integrity metric of the host operating system; and (c) supplying an integrity metric associated with the identified computing environment.

Preferably, the step (a) comprises receiving identity information associated with the computing environment, such as receiving information about a process running in a computing environment, and determining the computing environment which contains that process.

According to a third aspect of the present invention there is provided a computing platform, comprising: a host operating system; a plurality of computing environments each comprising a guest operating system running on the host operating system; and a trusted device for obtaining an integrity metric of the host operating system and an integrity metric of each computing environment.

Preferably, the trusted device stores the integrity metric for the host operating system and the integrity metric for each guest operating system. Preferably, the trusted device stores each integrity metric in a platform configuration register or a group of platform configuration registers. Preferably, the trusted device

allocates a platform configuration register or group of platform configuration registers to each computing environment.

5       For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings in which:

10       Figure 1 shows a preferred computing platform;

Figure 2 shows a preferred computing environment;

Figure 3 shows an example trusted device;

15

Figure 4 shows a preferred method for obtaining integrity metrics for multiple trusted computing environments;

20       Figure 5 shows a preferred method for verifying multiple trusted computing environments; and

Figure 6 shows a preferred computing platform communicating with a user.

25

Figure 1 shows a computing platform 20 employed in preferred embodiments of the present invention. The computing platform 20 comprises hardware 21 operating under the control of a host operating system 22. The hardware 21 may include standard features such as a keyboard, a mouse and a visual display unit which provide a physical user interface 211 to a local user of the computing platform. The hardware 21 also suitably

30

comprises a computing unit 212 comprising a main processor, a main memory, an input/output device and a file storage device which together allow the performance of computing operations. Other parts of the computing platform are not shown, such as connections to a local or global network. This is merely one example form of computing platform and many other specific forms of hardware are applicable to the present invention.

10 In the preferred embodiment the hardware 21 includes a trusted device 213. The trusted device 213 is suitably a physical component such as an application specific integrated circuit (ASIC). Preferably the trusted device is mounted within a tamper-resistant housing. The trusted device 213 is coupled to the computing unit 212, and ideally to the local user interface unit 211. The trusted device 213 is preferably mounted on a motherboard of the computing unit 212. The trusted device 213 functions to bind the identity of the computing platform 20 to reliably measured data that provides an integrity metric of the platform.

Preferably, the trusted device 213 performs a secure boot process when the computing platform 20 is reset to ensure that the host operating system 22 of the platform 20 is running properly and in a secure manner. During the secure boot process, the trusted device 213 acquires an integrity metric (or a group of integrity metrics) of the computing platform 20, such as by examining operation of the computing unit 212 and the local user interface unit 211. The integrity metrics are then available for a user to determine whether to trust the computing platform to operate in a predicted manner. In particular, a trusted

computing platform is expected not to be subject to subversion such as by a virus or by unauthorised access. The user includes a local user of the computing platform, or a remote user communicating with the computing platform  
5 by networking (including LAN, WAN, internet and other forms of networking).

WO 00/48063 (Hewlett-Packard) discloses an example computing platform suitable for use in preferred  
10 embodiments of the present invention. In this example the trusted device 213 acquires a hash of a BIOS memory of the computing unit 212 after reset. The trusted device 213 receives memory read signals from the main processor and returns instructions for the main processor to form the  
15 hash. The hash is stored in the trusted device 213, which then returns an instruction that calls the BIOS program and a boot procedure continues as normal.

Preferably, the trusted device 213 controls the local  
20 user interface 211 such that a local user can trust the display of data provided on a visual display unit. WO 00/73913 (Hewlett-Packard) discloses an example system for providing a trustworthy user interface by locating a driver for the visual display unit within the trusted  
25 device 213.

The hardware 21 may also comprise a trusted user interface for performing secure communication with a user device such as a smart card held by the user. The trusted  
30 user interface allows the user to perform trusted communications with the trusted device 213 in order to verify the integrity of the computing platform 20. The use of a smart card or other token for trusted user



interaction is described in more detail in WO 00/54125 (Hewlett-Packard) and WO 00/54126 (Hewlett-Packard).

Figure 1 shows a user 10 such as a remote client which  
5 is arranged to communicate with the computing platform 20, preferably over a secure channel 30. The secure channel 30 is protected, for example, using a shared session key, which is a secret which is known only to the computing platform 20 and the user 10. Providing a secure channel  
10 including generation of a shared session key will be familiar to the person skilled in the art. Ideally, the user 10 performs an integrity challenge to confirm that communication is made with an expected computing platform 20, using a signature provided by the trusted device 213.  
15 However, any suitable authentication can be employed.

The computing platform 20 provides a computing environment 24 which gives access to resources of the computing platform, such as processor time, memory area,  
20 and filespace. Preferably, a plurality of discrete computing environments 24 are provided. Each computing environment is logically distinct, but shares access to at least some of the resources of the computing platform with other computing environments.

25

Suitably, the computing environment 24 comprises a compartment. The actions or privileges within a compartment are constrained, particularly to restrict the ability of a process to execute methods and operations  
30 which have effect outside the compartment, such as methods that request network access or access to files outside of the compartment. Also, operation of the process within the compartment is performed with a high level of

isolation from interference and prying by outside influences.

Preferably, the compartment is an operating system  
5 compartment controlled by a kernel of the host operating  
system 22. This is also referred to as a compartmented  
operating system or a trusted operating system.

Compartmented operating systems have been available  
10 for several years in a form designed for handling and  
processing classified (military) information, using a  
containment mechanism enforced by a kernel of the  
operating system with mandatory access controls to  
resources of the computing platform such as files,  
15 processes and network connections. The operating system  
attaches labels to the resources and enforces a policy  
which governs the allowed interaction between these  
resources based on their label values. Most compartmented  
operating systems apply a policy based on the  
20 Bell-LaPadula model discussed in the paper "Applying  
Military Grade Security to the Internet" by C I Dalton and  
J F Griffin published in Computer Networks and ISDN  
Systems 29 (1997) 1799-1808.

25 The preferred embodiment of the present invention  
adopts a simple and convenient form of operating system  
compartment. Each resource of the computing platform which  
it is desired to protect is given a label indicating the  
compartment to which that resource belongs. Mandatory  
30 access controls are performed by the kernel of the host  
operating system to ensure that resources from one  
compartment cannot interfere with resources from another

compartment. Access controls can follow relatively simple rules, such as requiring an exact match of the label.

Examples of resources include data structures  
5 describing individual processes, shared memory segments, semaphores, message queues, sockets, network packets, network interfaces and routing table entries.

Communication between compartments is provided using  
10 narrow kernel level controlled interfaces to a transport mechanism such as TCP/UDP. Access to these communication interfaces is governed by rules specified on a compartment by compartment basis. At appropriate points in the kernel, access control checks are performed such as  
15 through the use of hooks to a dynamically loadable security module that consults a table of rules indicating which compartments are allowed to access the resources of another compartment. In the absence of a rule explicitly allowing a cross compartment access to take place, an  
20 access attempt is denied by the kernel. The rules enforce mandatory segmentation across individual compartments, except for those compartments that have been explicitly allowed to access another compartment's resources. Communication between a compartment and a network resource  
25 is provided in a similar manner. In the absence of an explicit rule, access between a compartment and a network resource is denied.

Suitably, each compartment is allocated an individual  
30 section of a file system of the computing platform. For example, the section is a chroot of the main file system. Processes running within a particular compartment only have access to that section of the file system. Through

kernel controls, the process is restricted to the predetermined section of file system and cannot escape. In particular, access to the root of the file system is denied.

5

Advantageously, a compartment provides a high level of containment, whilst reducing implementation costs and changes required in order to implement an existing application within the compartment.

10

Referring to Figure 1, it is desired to run a process 23 in one of the computing environments 24. In practical embodiments, many processes run on the computing platform simultaneously. Some processes are grouped together to form an application or service. For simplicity, a single process will be described first, and the invention can then be applied to many processes and to groups of processes.

20 Figure 2 shows a logical structure for a preferred computing environment 24 provided by the computing platform for running the process 23.

The process 23 runs on a guest operating system 25. 25 The guest operating system 25 is suitably provided by a virtual machine application 26. The virtual machine application 26 runs on the host operating system 22 and provides an image of a computing platform, or at least appropriate parts thereof. The virtual machine application 26 provides the virtual guest operating system 30 25 such that, as far as the process 23 is concerned, the process 23 runs on the guest operating system 25 equivalent to running on a host operating system 22.

For the purposes of the present invention, the guest operating system 25 is preferably a replica of the host operating system, or at least necessary parts thereof. However, it is equally possible for the virtual machine application 26 to provide a different emulated software or hardware environment, such as a different operating system type or version. An example virtual machine application is sold under the trade mark VMware by VMware, Inc of Palo Alto, California, USA.

10

The virtual machine application 26 assists security by isolating the process 23 from the remainder of the computing platform. Should problems occur during running of the process 23 or as a result thereof, the host operating system 22 can safely shut down the guest operating system 25 provided by the virtual machine application 26. Also, the virtual machine application 26 protects the host operating system 22 and hardware resources 21 from direct access by the process 23. Therefore, it is very difficult for the process 23 to subvert the host operating system 22. Further, the process 23 accesses resources of the computing platform made available through the virtual machine application 26. Each process 23 only sees resources of the computing platform allocated through the virtual machine application 26, such that a process 23 can be restricted to an appropriate share of the resource of the computing platform and cannot stop other processes having their allocated share.

30

Preferably, the virtual machine application 26 providing the guest operating system 25 runs in a compartment 220 of the host operating system 22. The

compartment confines communications and data access of the virtual machine application. The compartment 220 provides secure separation between applications, such that processes are inhibited from communicating with each other, accessing each others status, or interfering with each other, except in accordance with strictly enforced access controls. In particular, a compartment assists the virtual machine application in resisting subversion by a process running in that computing environment.

10

Referring again to Figure 2, the process 23 runs in the computing environment 24. It is desired to confirm the integrity of this computing environment. Also, many similar computing environments can be provided on the computing platform simultaneously, and it is desired to confirm the integrity of one selected computing environment independently of the integrity of any other computing environment. That is, it is desired that the multiple computing environments are independently trustworthy. Advantageously, the use of a guest operating system 25, preferably in combination with a compartment 220, provides a high degree of isolation between computing environments, such that the integrity of one computing environment is not affected by activity in any other computing environment.

25

As described above, the trusted device 213 is arranged to form an integrity metric (or a group of integrity metrics) of the host operating system 22. Also, in the preferred embodiments of the present invention, the trusted device 213 is arranged to obtain an integrity metric (or a group of integrity metrics) for each computing environment 24. Preferably, the trusted device

30

213 obtains an integrity metric of the guest operating system 25. Further, the trusted device preferably obtains an integrity metric of the virtual machine application 26. Each integrity metric suitably comprises one or more  
5 separate integrity metric values.

In the preferred configuration the host operating system 22 has direct access to the trusted device 213. However, to improve security, processes (i.e.  
10 applications) running on the host operating system 22 do not have direct access to the trusted device 213. Therefore, a trusted device driver 221 is provided, suitably as part of the host operating system 22. The trusted device driver 221 provides an interface available  
15 to applications running on the host operating system 22, including allowing results to be reported to the trusted device 213, and allowing stored integrity metric values to be obtained from the trusted device 213.

20 Figure 3 shows a simplified example of the preferred trusted device 213. Amongst other components the trusted device 213 comprises an addressable storage such as a plurality of platform configuration registers (PCRs). In this example eight PCRs are shown, namely PCR\_0 to PCR\_7  
25 although in practice many more PCRs are available. Suitably, each PCR stores a digest such as a 160 bit hash value representing an integrity metric 231. A group of PCRs form a group of integrity metrics 230. Suitably, the trusted device driver 221 allocates a PCR, or a group of  
30 PCRs, to the or each computing environment 24. Therefore, information concerning the integrity of each computing environment is independently available from the trusted device 213.

The stored integrity metric value 231 preferably represents a sequence of integrity metric values obtained, for example, by examination of the host platform 20 periodically or in response to relevant events. The old stored integrity metric value is combined with a new integrity metric value to produce a new updated digest of the sequence of values.

10        Figure 4 shows a preferred method for obtaining integrity metrics of a computing platform for providing multiple trusted computing environments.

         In step 401, the host operating system 22 is provided. Suitably, this includes the steps of starting a BIOS, starting an OS loader, and starting the host operating system as will be familiar to the skilled person.

         In step 402, a group of integrity metrics 230 for the host operating system 22 are measured and reported to the trusted device 213. Preferably, the trusted device 213 obtains an integrity metric for the BIOS, and preferably also obtains an integrity metric for the OS loader and the operating system software. Preferably, integrity metric values relevant to the host operating system are stored in a group of PCRs (or other addressable storage) such that the integrity metrics 230 for the host operating system are available later. Steps 401 and 402 are shown separately for clarity. In practical embodiments of the invention it will be appreciated that the integrity metrics 230 are obtained concurrently with providing the host OS 22.



Optionally, at step 403 additional integrity metrics are obtained relevant to other selected elements of the computing platform. For example, the trusted device 213 performs data event logging as described in WO 00/73880  
5 (Hewlett-Packard). Also, the trusted device 213 may produce a digest by applying a hash function to all or selected data files stored on the computing platform, as described in WO 00/73904 (Hewlett-Packard). Preferably, at least some of the integrity metrics obtained in step  
10 402 or step 403 are updated periodically or in response to relevant events to confirm the current integrity status of the host operating system and related components of the computing platform.

15 In step 404, a guest operating system 25 is provided, to form a new computing environment 24. Suitably, step 404 includes providing a virtual machine application 26 which provides the guest operating system 25.

20 Preferably, the step 404 includes providing the guest operating system 25 in a compartment 220 of the host operating system 22. Also, the step 404 preferably includes providing a history of all processes (applications) launched in the compartment. Here, it is  
25 desired to record whether any other applications have been launched alongside the virtual machine application 26 which provides the guest operating system 25.

In step 405, the trusted device 213 obtains an  
30 integrity metric for the computing environment 24. In particular, the trusted device 213 obtains an integrity metric or group of integrity metrics 230 for the guest operating system 25, and preferably the virtual machine

application 26. The corresponding integrity metric values  
231 are stored in a PCR or group of PCRs allocated to that  
computing environment.. Also, the step 405 preferably  
includes obtaining an integrity metric for the or each  
5 process 23 in the computing environment. Suitably, each  
integrity metric is obtained by forming a digest (hash  
value) of program code of a process. As will be familiar  
to the skilled person, the term integrity metric can refer  
to a single data item, or can refer to a metric formed  
10 from two or more parts each of which themselves can be  
considered an integrity metric.

Preferably, step 405 is repeated such that a current  
integrity status of the computing environment is available  
15 and history information is updated, periodically or in  
response to a relevant event.

When it is desired to create or update a stored  
integrity metric for a particular computing environment, a  
20 result is reported to the trusted device driver 221 along  
with information identifying that particular computing  
environment, such as an arbitrary label. In one preferred  
embodiment a process ID of the virtual machine application  
26 is used to identify the computing environment. In  
25 another embodiment each logical computing environment is  
supplied with a secret, e.g. a secret is supplied to the  
virtual machine application 26 by the trusted device  
driver 221, and then the secret is subsequently used to  
identify the computing environment. Suitably the computing  
30 environment label, such as a secret, is supplied by the  
host OS 22 when the virtual machine application 26 is  
launched.

Referring to Figure 5, a preferred method for verifying a computing environment will now be described.

Optionally, in step 501 a secure channel is  
5 established for communicating with the computing platform 20. For a local user 10, a secure channel is provided such as by using a trustworthy user interface and/or by using a token such as a smart card. A remote user 10 establishes a secure channel 30 such as by performing  
10 authentication of the computing platform, ideally using a signature from the trusted device 213. Here again, the user optionally employs trusted hardware, such as the user's own client platform, a PDA, mobile phone or other device, optionally in co-operation with a smart card or  
15 other token. Preferably, the step 501 includes establishing the authentication and authorisation of the user.

In step 502, the user 10 requests demonstration of the  
20 integrity of a computing environment 24. For example, the user 10 issues an integrity challenge. To avoid a re-play attack, the challenge suitably includes a random number sequence (nonce). More detailed background information is provided in "TCPA Specification Version 1.0" published by  
25 the Trusted Computing Platform Alliance.

In step 503 the trusted device 213 supplies integrity metrics associated with the host operating system 22. Suitably, these integrity metrics include integrity  
30 metrics for the BIOS, operating system loader and host operating system, and integrity metrics formed by periodic or event-driven checks on the host operating system and related components of the computing platform.

In step 504, the trusted device 213 supplies an integrity metric associated with the selected computing environment. Preferably, the step 504 includes supplying  
5 integrity metrics associated with the virtual machine application 26, the guest operating system 25, the process 23, and a history of periodic or event-driven checks made on the integrity status of the computing environment 24.

10 The step 504 preferably includes supplying a history of any applications launched by the host operating system in the same compartment as the guest operating system, i.e. alongside the virtual machine application 26.

15 Preferably, in step 505 the integrity metric for the host operating system 22 and the computing environment 24 are compared against expected values, such as by using a certificate issued by a trusted party that is prepared to vouch for the integrity of the computing platform. If the  
20 comparison is successful, the computing environment is considered to be a trusted computing environment.

Figure 6 shows the preferred computing platform of Figure 2 communicating with a user 10, to perform the  
25 method of Figure 5. As discussed above in step 502, the user 10 issues a request for verification of the integrity of a computing environment 24, suitably in the form of an integrity challenge.

30 In a first example, the integrity challenge is issued direct to a component of the host operating system 22, such as the trusted device driver 221. In this embodiment, the integrity challenge includes information

previously given to the user 10, such as an arbitrary label, which allows the trusted device driver 221 to establish the relevant computing environment 24. The external computing environment identity label given to the user 10 may be the same as, or complementary to, any information held internally identifying the computing environment. Suitably, the external identity information supplied as part of the integrity challenge is matched against a list of computing environments currently provided on the host operating system, this step ideally being performed by the trusted device driver 221. Suitably, there is a one to one relationship between the compartment identity label as given to the user 10, and any compartment identity label used internally in the host computing platform 20. In step 504 the trusted device 213 supplies an integrity metric or group of integrity metrics 230 associated with the identified computing environment 24.

In a second preferred example, the integrity challenge is issued from the user 10 and is received by a component of the relevant computing environment 24, such as the process 23 which suitably forms part of an application running in that computing environment 24. The integrity challenge is passed from the computing environment 24 to the trusted device driver 221. In this case, the trusted device driver 221 can readily establish the identity of the computing environment 214 passing the integrity challenge. In one example embodiment the computing environment 24 supplies an internal computing environment identity label such as a process ID of the virtual machine application 26, or a secret previously given to the virtual machine application 26 by the host operating

system 22. In step 504 the trusted device 213 supplies integrity metrics associated with that computing environment 24.

5 In a further preferred aspect that can be applied to any of the methods described herein, the guest operating system 25 is itself a compartmented operating system. Multiple applications can be run on the guest operating system 25, each within a separate compartment of the guest  
10 operating system. This embodiment enables each computing environment 24 to be subdivided, and the method described above is applied to the subdivided computing environments.

Advantageously, a trusted computing environment is  
15 provided by using a trusted device to verify that a guest operating system has booted in a trusted manner. By repeating this process and running multiple guest operating systems, multiple trusted computing environments are provided. A first application can run in a first of  
20 the computing environments, whilst a second application can run in a second of the computing environments, where the first and second applications are mutually incompatible or one does not trust the other. The preferred implementation using a virtual machine  
25 application in combination with a compartment allows each computing environment to be independently trusted.

It is very difficult for a process running in one computing environment to affect the integrity of any other  
30 computing environment. Advantageously, a user can verify the integrity of one computing environment without reference to the integrity of any other computing environment. In the preferred implementation each

computing environment has an associated set of one or more integrity metrics which do not include or depend on information about any other computing environment.

**Claims**

1. A method for providing a trusted computing environment, comprising the steps of:

5

(a) providing a host operating system;

(b) obtaining an integrity metric for the host operating system;

10

(c) providing a computing environment including a guest operating system; and

(d) obtaining an integrity metric for the computing environment.

15

2. The method of claim 1, wherein the step (b) includes obtaining the integrity metric during boot of the host operating system.

20

3. The method of claim 2, wherein the step (b) includes obtaining an integrity metric for a BIOS and/or an OS loader and/or an operating system software of the host operating system.

25

4. The method of claim 1, wherein the step (b) includes obtaining the integrity metric by performing data event logging, and/or by performing a hash function to all or selected data files associated with the host operating system.

30



5. The method of claim 1, wherein the step (b) comprises updating at least part of the integrity metric for the host operating system.

5 6. The method of claim 1, wherein the step (d) comprises obtaining an integrity metric of the guest operating system.

7. The method of claim 1, wherein the step (c)  
10 comprises providing a virtual machine application running on the host operating system for providing the guest operating system.

8. The method of claim 7, wherein the step (d)  
15 comprises obtaining an integrity metric of the virtual machine application.

9. The method of claim 1, wherein the step (c)  
comprises providing a process running on the guest  
20 operating system.

10. The method of claim 9, wherein the step (d) comprises obtaining an integrity metric of the process.

25 11. The method of claim 1, wherein the step (c) comprises providing the computing environment in a compartment of the host operating system.

12. The method of claim 11, wherein the host operating  
30 system is a compartmented operating system.

13. The method of claim 11, wherein the compartment confines the guest operating system.

14. The method of claim 11, wherein the step (d) comprises obtaining an integrity metric from a history of all processes launched in the compartment.

5

15. The method of claim 1, wherein the step (d) comprises updating at least part of the integrity metric for the computing environment.

10 16. The method of claim 1, wherein the step (b) comprises storing the integrity metric for the host operating system, and/or the step (d) comprises storing the integrity metric for the computing environment.

15 17. The method of claim 16, wherein the integrity metric for the computing environment is stored associated with an identity of the computing environment.

18. The method of claim 1, wherein the step (b) and/or  
20 the step (d) comprises obtaining the integrity metric using a trusted device.

19. The method of claim 18, comprising storing each integrity metric in a platform configuration register of  
25 the trusted device.

20. The method of claim 19, comprising storing the integrity metric for the computing environment in a platform configuration register or group of platform  
30 configuration registers associated with the computing environment.

21. The method of claim 1, comprising the step of verifying the trusted computing environment including the steps of:

5 (e) identifying the computing environment;

(f) supplying the integrity metric for the host operating system; and

10 (g) supplying the integrity metric for the computing environment.

22. The method of claim 1, wherein the step (c) comprises providing a plurality of computing environments  
15 each including a guest operating system, and the step (d) comprises obtaining an integrity metric of each computing environment.

23. A method for verifying integrity of a trusted  
20 computing environment amongst many on a single host computing platform running a host operating system, each computing environment comprising a guest operating system running on the host operating system, the method comprising the steps of:

25 (a) identifying the computing environment;

(b) supplying an integrity metric of the host operating system; and

30 (c) supplying an integrity metric associated with the identified computing environment.

24. The method of claim 23, wherein the step (a) comprises receiving identity information associated with the computing environment.

5 25. The method of claim 24, comprising receiving information about a process running in a computing environment, and determining the computing environment which contains that process.

10 26. A computing platform, comprising:

a host operating system;

a plurality of computing environments each comprising  
15 a guest operating system running on the host operating system; and

a trusted device for obtaining an integrity metric of the host operating system and an integrity metric of each  
20 computing environment.

27. The computing platform of claim 26, wherein the trusted device stores the integrity metric for the host operating system and the integrity metric for each guest  
25 operating system.

28. The computing platform of claim 27, wherein the trusted device stores each integrity metric in a platform configuration register or a group of platform  
30 configuration registers.

29. The computing platform of claim 28, wherein the trusted device allocates a platform configuration register

or group of platform configuration registers to each computing environment.

30. A method for providing a trusted computing  
5 environment, substantially as hereinbefore described with reference to Figure 4 of the accompanying drawings.

31. A method for verifying integrity of a trusted  
10 computing environment amongst many on a single host computing platform running a host operating system, each computing environment comprising a guest operating system running on the host operating system, substantially as hereinbefore described with reference to Figure 5 of the accompanying drawings.

15

32. A computing platform substantially as hereinbefore described with reference to Figures 1 and 2 of the accompanying drawings.

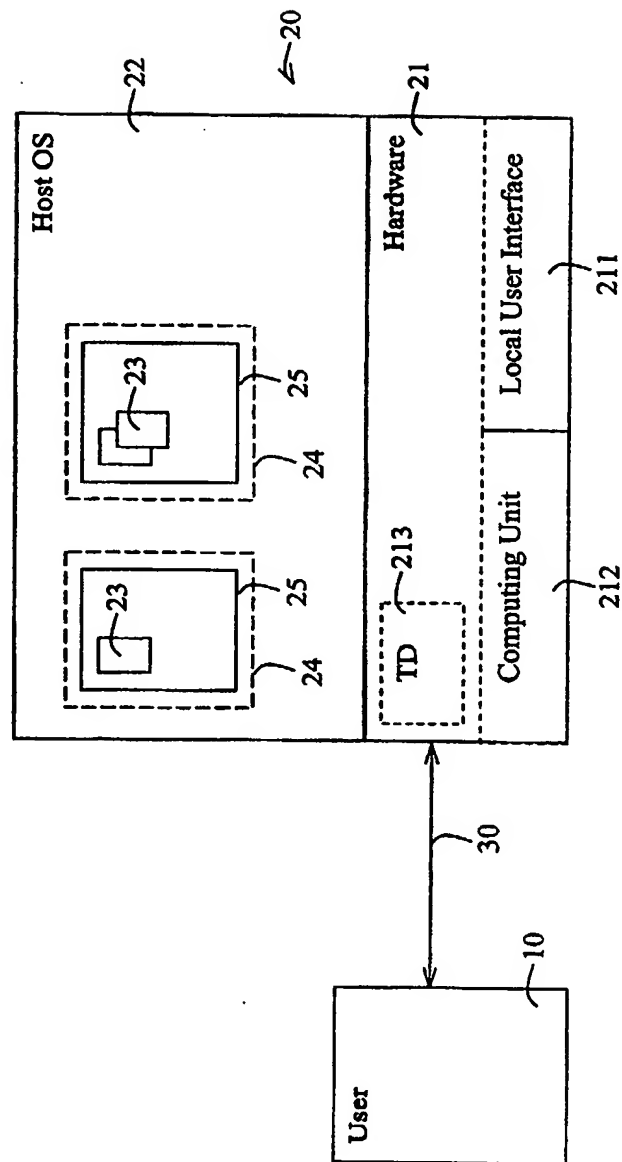
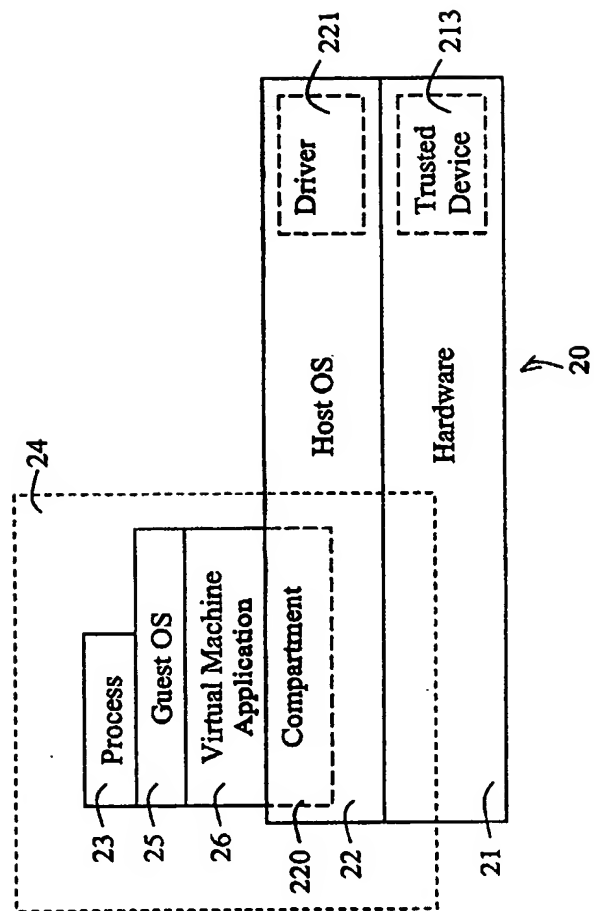


Fig. 1



**Fig. 2**

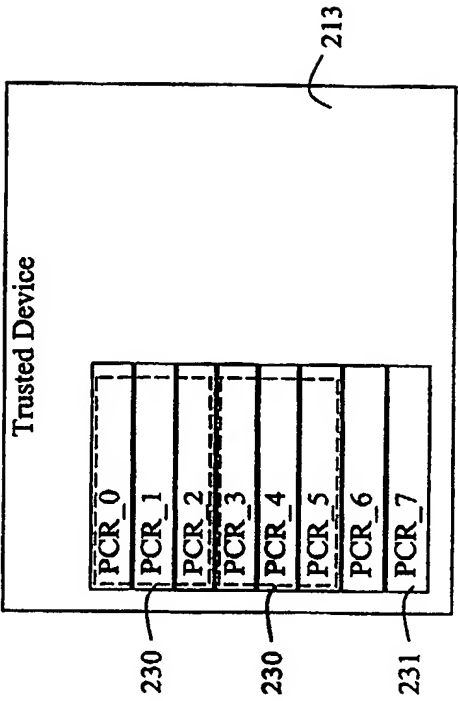
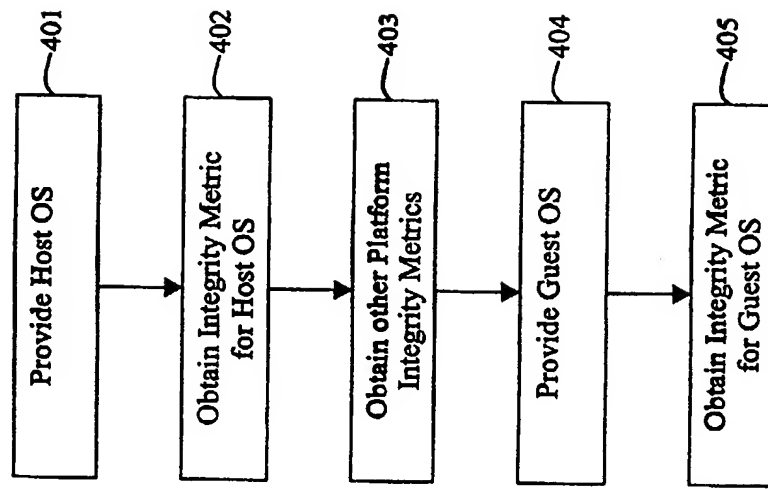
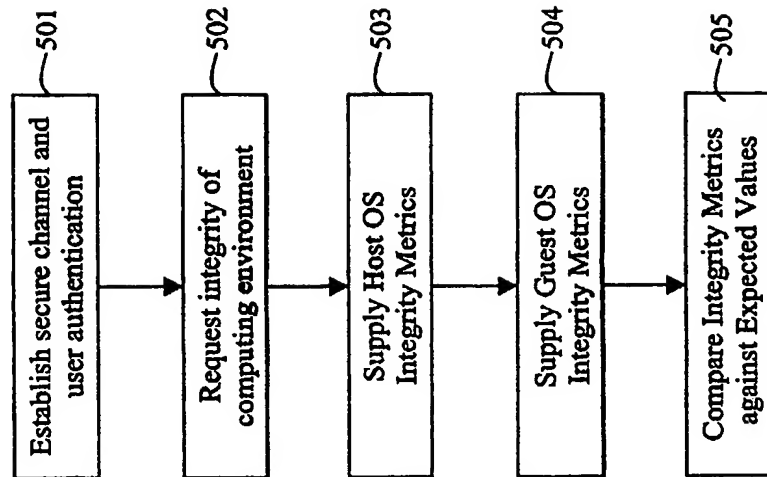


Fig. 3



**Fig. 4**

**Fig. 5**

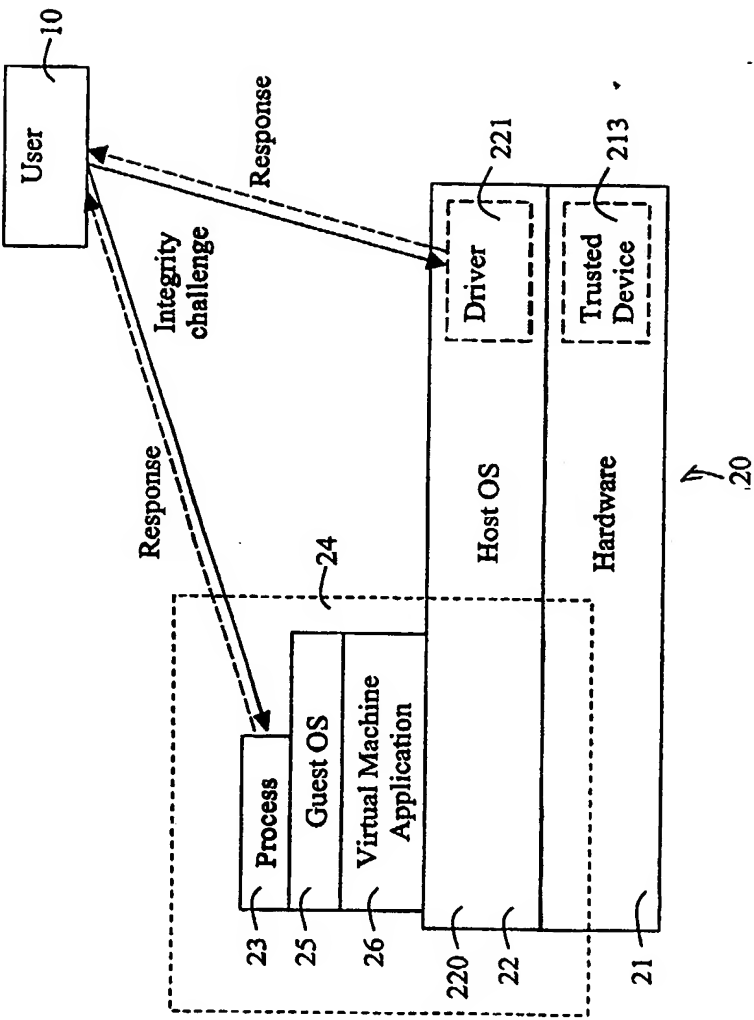


Fig. 6



Application No: GB 0114891.5  
Claims searched: 1-32

Examiner: D Midgley  
Date of search: 28 February 2002

## Patents Act 1977 Search Report under Section 17

### Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A AAP

Int Cl (Ed.7): G06F 1/00,9/455,12/14

Other: ONLINE:WPI,EPODOC,JAPIO,TDB,INSPEC,XPESP

### Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	EP 1030237 A1 (HEWLETT PACKARD)	1,23 and 26
A	WO 00/48063 A1 (HEWLETT PACKARD)	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.